アクセス管理フェデレーションに基づいた複数の SAML 対応ミドルウェアを使用した学術コンテンツのための共有サービスの開発

伊藤智博[†1]　立花和宏[†1]　奥山澄雄[†1]　高野勝美[†1]
田島靖久[†1]　吉田浩司[†1]　仁科辰夫[†1]

シングルサインオンは，認証プロバイダーとサービスプロバイダーの連携によって実現できる．サービスプロバイダーの SAML 対応ミドルウェアとしては，Microsoft 社が提供する ADFS や Shibboleth コンソーシアムが提供する Shibboleth がある．本研究では，これらの 2 つのミドルウェアを活用して，学術コンテンツのための共有サービスを開発した．市販のグループウェアである SharePoint サーバを ADFS によって学認に対応した．典型的なコラボレーションサービスは，SharePoint サーバ使用して，低い運用コストで学認に提供した．スキーマや数値の共有を目的する研究型コンテンツサーバは，Shibboleth によって学認に対応した．SharePoint サーバと研究型コンテンツサーバは相互リンクによって，低コストで拡張可能な共有システムの構築を可能にした．さらに，SAML 対応ミドルウェアによるシングルサインオンによって，システムの利便性を向上した．

Development of sharing service for science contents using multiple SAML middleware based on access management federation

TOMOHIRO ITO[†1]　KAZUHIRO TACHIBANA[†1]　SUMIO OKUYAMA[†1]
KATSUMI TAKANO[†1]　YASUHISA TAJIMA[†1]　HIROSHI YOSHIDA[†1]
TATSUO NISHINA[†1]

In a federated authentication, single sign-on (SSO) for web applications can be achieved by performing authentication at identity provider (IdP) and authorization at the service provider (SP). There are the Shibboleth and the ADFS as a typical SAML middleware for the service provider. This study developed the sharing system of science information using multiple SAML middleware based on access management federation. The commercial collaboration software of SharePoint server corresponded to the Gakunin by using ADFS. Typical collaboration service was provided for the Gakunin at a low-operation-cost by using the SharePoint server. The research type contents server for sharing of the schemata and numerical values corresponded to the Gakuniun by using Shibboleth. The extendible sharing system was constructed low-cost by using mutually hyperlink of SharePoint server and research type contents server, and this system has improved the convenience by using single-sign-on based on the SAML middleware.

1. はじめに

近年，ネットワークやデータベースなど様々なサービスにおいて，セキュリティレベルの維持を目的として，何からの認証を求めることが当たり前となってきている．一方で，様々なシステムに異なるアカウントが発行されたことにより，利用者が複数のパスワードなどの認証情報を暗記するなどの利用者への負担が増大した．この問題を解決するために，複数のアプリケーションへのログイン処理が簡素化されるシングルサインオンの導入が必要不可欠であった．

本学のシングルサインオン導入の経緯を説明しますと，2003 年の時点では，本学の各部局や部署がシステム毎に独自のアカウントを発行していたため，多くのアカウントが存在し様々なトラブルの原因となっていた．情報系センター（当時の情報処理センター；以下センター）のアカウントですら，UNIX 系と Windows 系で独立しており，パスワードの取り扱いが複雑になる問題が生じていた．また，山形大学は，4 つからなる分散キャンパスであるため，運用方針についても，キャンパス毎に異なる要望があり，その要望に応えるため，様々な運用形態が生まれ複雑化していた．2004 年度より，工学部が設置されている米沢キャンパスのセンターが中心になって，認証統合の技術的な解決策と試行運用が開始された．検証課題として，「デジタル証明書」，「UNIX 系と Windows 系のパスワード同期」，「ネットワーク装置からの Active Directory(AD)への認証」，「オブジェクト識別子(OID)の設計」，「複数認証基盤の連携」を掲げ，それぞれの課題の技術面及び運用面での解決が試みられた．2005 年には，全ての課題について，問題解決がなされ，工学部の利用者は，センターが提供するリソースに対して，1 つのアカウントで全てのサービスを利用できるようになった．その後，80 番ポートを介在して増殖するワームの対策の 1 つとして，工学部では，外部接続時にネットワーク利用者認証を必須とする運用方針が適用され、アカウントの

†1 山形大学
Yamagata University

利用者数は，米沢キャンパスのネットワーク利用者数である約 4000 人へと増加した．また，2007 年に実施した教育用実習システムの更新では，全てのキャンパスに米沢キャンパスと同様の統合認証を導入した．これによって，全学の利用者は，センターが提供する全てのサービスがシングルサインオンで利用できるようになった．

教務システムや会計システムなどの業務系のシステムとの認証の統合については，様々な議論の結果，センターが中心となって運用している学術系の認証情報とは統合しないという結論に至った．議論の内容を要約すると，教育・研究現場では，学問の自由が許されている．一方，業務システムでは，堅牢なセキュリティシステムが必要とされる．この 2 つのポリシーは、互いに相反するため，その両方を同一の認証基盤で円滑に運用することは，困難であると判断した．すなわち，山形大学では，センターが管理・提供する「教育研究用認証基盤」と事務が中心となって管理・提供する「業務系認証基盤」のセキュリティレベルが異なる 2 つのアカウントが存在する．

2006 年度から，国立情報学研究所(NII)及び全学共同利用情報基盤センターが中心となり，全国大学共同電子認証基盤構築事業（UPKI：University Public Key Infrastructure）を 3 年計画で実施した[1]．この事業では，各大学にある計算機資源や情報インフラなどを大学間で，シームレスかつ安全に活用すること目的して，「デジタル証明書」，「グリッドコンピューティング」，「証明局」，「シングルサインオン」，「無線 LAN ローミング」を中心に認証基盤のプロトタイプ試験を実施した．

2008 年度には，UPKI 認証連携基盤実現のために技術的及び制度的な検証を行うために，「UPKI 認証連携基盤によるシングルサインオン実証実験（SSO 実証実験）が実施された．山形大学では，分散キャンパスで円滑に認証連携を進めるための技術的なノウハウを蓄積することを 1 つの目的として，LDAP プロキシや Radius プロキシによる複数認証基盤を統合し，SSO 実証実験及び大学間無線 LAN ローミング eduroam (eduroam)に参加した[2][3]．2009 年には，UPKI-学術認証フェデレーションの試行運用フェデレーション（現在の学術認証フェデレーション；以下学認）に参加し，本格的な利用者サービスを開始した[4]．Shibboleth (シボレス)認証は，東日本大震災が発生した際に，本学の安否確認システムを 6 時間程度で構築できることから，開発コストを軽減できるツールの 1 つであった[5]. 2011 年には，東日本大震災を踏まえて，複数 ISP と分散認証データベースによる高可用性認証連携システムを構築し，学認をはじめとする様々なフェデレーションとの認証連携機能の可用性を向上した[6][7].

現在，代表的な SAML 対応ミドルウェアとしては，Microsoft 社が提供する Active Directory Federation Service(ADFS)と Shibboleth コンソーシアムが提供する Shibboleth が存在する．もし，この 2 つのミドルウェアを組み合わせてサービス展開を行うことができれば，それぞれの持ち味を活かし，低コストでサービスプロバイダーを開発できることが期待される．本研究では，この 2 つのミドルウェアを活用した学術コンテンツのための共有サービスの開発について報告する．

2. サービスの全体設計と情報機器

2.1 サービスの設計

教育・研究現場で，共有サービスが取り扱うコンテンツには，2 種類に分類される．1 つ目は，予定表，ファイル，テキスト，アンケートなどの市販のグループウェアを用いて代用可能な定型的なコンテンツである. 2 つ目は，数字，スキーマ，計算式などの定型化されない研究型のコンテンツである．

定型的なコンテンツは，市販のグループウェアを使用することによって，低い開発コストで共有サービスを提供でことが期待される．一方，研究型コンテンツは，市販のグループウェアでは対応することが難しい．たとえば，研究型コンテンツが取り扱うオブジェクトとしては，元素や化学種，単位操作，反応式，計算式，物理量，研究ノート，試料などがある．これらのオブジェクトをデータベースに蓄積し，相互に関連付けることによって，データベースによる学問の体系化を目指すことにした．しかし，これらのオブジェクトを取り扱い，さらに，関連付けることができるデータベースやウェブアプリケーションは，存在しない．すなわち，研究型コンテンツを取り扱うデータベースウェブアプリケーションは，大学などの研究機関が開発し，学問領域の発展による多様な変化に対応し続けることが重要であろう．

このような現状を踏まえて，図 1 に示すような学術コンテンツ共有サービスを設計した．定型的なコンテンツは，グループウェアの 1 つである Microsoft 社製の SharePoint Foundation Server 2010(SharePoint)を使用して，定型的なコンテンツ用の共有サービスを提供することにした．研究型コンテンツは，匿名ユーザへの公開情報と認証ユーザへのグループ共有情報の 2 つの情報を管理できるサービスとした．ユーザ認証には，学認ログインを使用した．利用者のフロントエンドウェブサーバとして，「公開用ウェブサーバ」，「学認用ウェブサーバ」，「SharePoint サーバ」の 3 つを構築した．詳しくは後述するが，SharePoint サーバのみでは学認に対応できないため，学認の SAML アサーションを WS-Federation の SAML アサーションに変換するための ADFS サーバを別途構築する必要があった．バックエンドデータベースには，データベースミラーなどによる高可用性や多次元分析機能を有する Microsoft SQL Server 2008 R2 Enterprise Edition を使用した．フロントエンドウェブサー

バ間は，相互にハイパーリンクを設定できることで，それぞれのサーバ間を移動しながら，円滑な情報共有を実現することにした.

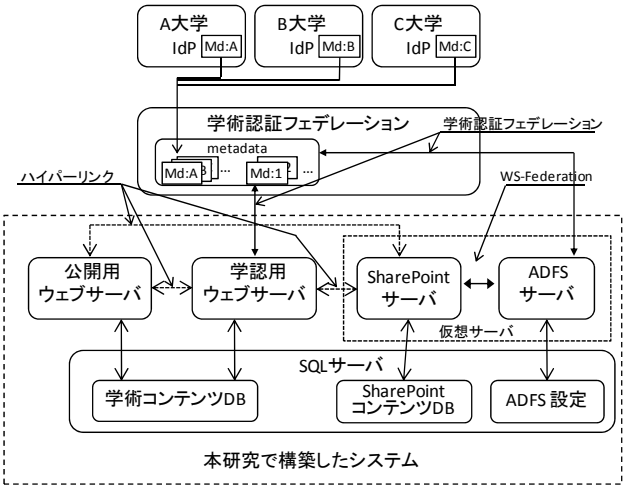

図 1　学術コンテンツ共有サービスの概略

2.2 使用した情報機器

サービスの実運用において，公開用ウェブサーバ，学認用ウェブサーバ，ADFS サーバ，SharePoint サーバ，SQL サーバを使用した. 学内の認証基盤は, Windows Server 2008 上の AD サービスによって提供されている. 仮想サーバは，ADFS サーバ，SharePoint サーバをはじめとする 25 のゲストマシーンが動作している．今後，新しいサービスを展開することを想定し, 40 程度のゲストマシーンを動作できるように設計した．SQL サーバは，研究やログの解析にも利用されおり，現在, 約 1500 万件／日のトランザクションを処理している．導入時に，2 億件／日のトランザクションを処理できるように設計した．以下に，それぞれのサーバのスペックを示す.

[仮想サーバ]
CPU: AMD Opteron 6180SE 2.5GHz ×4
メモリ: 128 GB
ローカル HDD: 1.8 TB
共有 HDD: 10 TB
OS: VMware vSphere 5.0 Enterprise Plus
備考：冗長性を保つために，複数の物理サーバで構成

[ADFS サーバ]
CPU:2 (仮想サーバ上で動作)
メモリ：4GB
HDD: 90 GB
OS: Microsoft Windows Server 2008 R2 Enterprise Edition
アプリケーション: ADFS 2.0, Visual Studio 2008 Professional

[SharePoint サーバ]
CPU:2 (仮想サーバ上で動作)
メモリ: 4GB
HDD: 128 GB
OS: Microsoft Windows Server 2008 R2 Standard Edition
アプリケーション：SharePoint Foundation Server 2010

[SQL サーバ]
CPU: AMD Opteron 6282SE 2.6GHz ×2
メモリ：64GB
HDD: 3.6TB (900GB×8, RAID 6)
OS: Microsoft Windows Server 2008 R2 Enterprise Edition
アプリケーション: Microsoft SQL Server 2008 R2 Enterprise Edition

[公開用ウェブサーバ]
CPU: Intel Celeron Processor G530 2.4GHz
メモリ：4GB
HDD: 250GB (250GB×2, RAID 1) + 160GB
OS: Microsoft Windows Server 2008 R2 Standard Edition
アプリケーション： Web アプリケーション(ASP .NET 4.0)

[学認用ウェブサーバ]
CPU: Intel Celeron Processor G530 2.4GHz
メモリ：4GB
HDD: 250GB (250GB×2, RAID 1) + 160GB
OS: Microsoft Windows Server 2008 R2 Standard Edition
アプリケーション： Web アプリケーション(ASP .NET 4.0)
Shibboleth SP 2.4.3

[開発用パソコン]
CPU: Intel Xeon E3-1230×1
メモリ：12GB
HDD: 250GB
OS: Microsoft Windows 7 Professional
アプリケーション： Visual Studio 2010 Professional, Internet Explorer 9, Firefox 13.0, Microsoft Access 2010

3. 構築

3.1 SharePoint サーバの問題点と解決策

学認対応 SharePoint サーバの構築については，既に詳細を報告しているので，本論文中では，問題点と概要について説明する[8].

SharePoint サービスを学認に対応するためには, 2 つの大きな問題点を解決する必要がある．1 つ目の問題点は，SharePoint サービスが提供する SAML ベースの認証方式であるクレームベース認証は，学認が推奨する Shibboleth と

直接連携が難しいことである．2 つ目の問題点は， ADFS は，学認が提供するような複数の認証プロバイダ(IdP)やサービスプロバイダ(SP)の信頼情報を 1 つのファイルに集約したメタデータを直接読み込めないことである．この 2 つの問題を解決するために，図 2 に示すようなシステムを構築した．1 つ目の問題点は，ADFS サーバがシボレス IdP からの SAML アサーションを WS-Federation 用の SAML アサーションに変換する認証ゲートウェイのような機能を利用することで解決した．2 つ目の問題点は，学認が提供するメタデータを読み込み解析する XML リーダモジュールを開発し，ADFS に対応したメタデータに変換し，読み込ませることで解決した．特に，ADFS サーバは，メタデータの読み込みための登録用スクリプトと IdP 毎のメタデータが必要であり，それらの情報は全て公開用ウェブサーバからダウンロードできるようになっている．すなわち，本学の研究室や他大学が ADFS を使用してサービスプロバイダーを構築する場合，センターが提供する ADFS 用メタデータ変換サービスを利用できるようになっている．

SharePoint サービスを利用するためには，個人を識別するための個人識別子を使うことが必須になっている．また，グループ属性も利用できるようになっており，山形大学の構成員にのみに，書き込み権限を与えることができるなどのメンバー管理機能を有している．これらのことを踏まえて検討した結果，山形大学が学認に提供している SharePoint サービスは，

・個人識別子は，mail 属性(0.9.2342.19200300.100.1.3)

・グループ識別子は，ePSA 属性(1.3.6.1.4.1.5923.1.1.1.9)

に対応している．

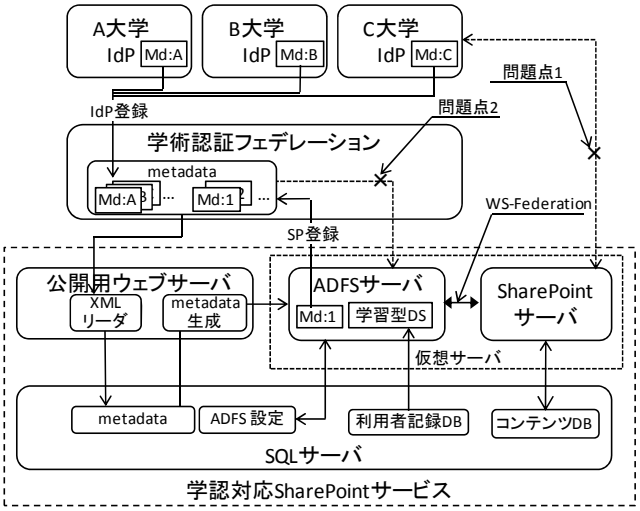

図 2 学認対応 SharePoint サービスの概略

3.2 研究型コンテンツサーバの設計とセキュリティ

研究型コンテンツサービスは，図 3 に示すように公開用と学認用の 2 つのウェブサーバによって提供される．アプリケーションの開発コストの軽減のために，公開用ウェブサーバと学認用ウェブサーバの実行コードは同一のもので動作するようにした．具体的な機能追加の手順について説明すると，開発者は，開発用パソコン内の Visual Studio 2010 を使用して，開発用ウェブサーバ内になるソースコードを編集して，アプリケーションに機能を追加する．機能を追加されたアプリケーションは，開発用ウェブサーバを使用して，デバッグ・動作確認などを行いながら修正が繰り返しながらプログラムの完成度が高められる．完成したアプリケーションは，リリースビルドを行い，学認用ウェブサーバに実行コードのみを発行する．学認用ウェブサーバに発行された実行コードは，分散ファイルシステム (Distributed File System; DFS)のレプリケーション機能により，公開サーバに転送される．各ウェブサーバでは，Internet Information Services(IIS)が同一のアプリケーションプログラムを読み込み，機能追加後のウェブサービスを提供できるようになる．また，各ウェブサーバは，同一の SQL サーバに接続し，コンテンツデータベースの格納された共通の情報を発信できるようになっている．

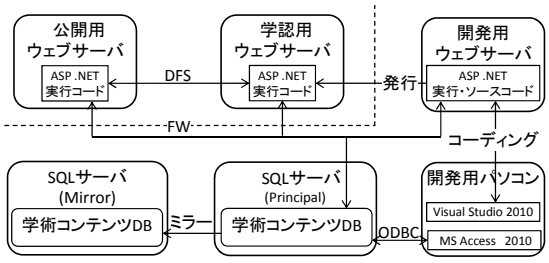

図 3 研究型コンテンツサーバの概略と構成

アプリケーションのコーディングの負担を軽減するために，オブジェクト指向の言語を利用して，表 1 に示すようなクラスの階層化構造を導入した．階層化構造を導入したことによって，派生クラスから基本クラスで定義されたメソッドやプロパティを再帰利用できるため，コードの短縮化とメンテナンス性の向上が期待される．また，派生クラス内で基本クラスに定義されたメソッドの機能を変更したい場合は，メソッドをオーバーライドすることによって，柔軟な拡張性を保つことも可能である．オブジェクト指向のコード設計によって，新しいデータベースのテーブルを追加するとき，10 行程度のコードの記述によって基本的な機能を動作できるようになった．

本サービスを構築するために必要不可欠な利用者の認証情報判別する機能は，html_tool クラスに記述されており，公開用または学認用ウェブサーバを識別し，適切なセキュリティを保つようにしてある．学認用ウェブサーバの SAML ミドルウェアは Shibboleth SP を使用した．Shibboleth SP は，受信した SAML アサーションを Header 情報として，IIS サーバに渡すようになっている．html_tool クラスには，IIS サーバから取得して Header 情報を解析し，SQL サーバ内に定義されている権限テーブルと照合し，アプリケーションのセキュリティを保つようになっている．

表 1　クラスライブラリーの例

クラス名	基本クラス	概要
Root	なし	固有な ID を取り扱うクラス（基底クラス）
html_tool	Root	Web サービスに関する環境変数や認証処理を行うクラス
sql_tool	html_tool	SQL 言語によるクエリー前処理を記述したクラス
Hypertext	sql_tool	html 言語によるタグの処理に関するクラス
Database	Hypertext	SQL 言語のクエリーの生成や ODBC による接続手順を定義するクラス
(対象のクラス名)	Database	データベースのテーブル固有のオブジェクトの処理を記述するクラス(例: Atom)
(web_page)	System.Web.UI 配下のクラス	ユーザがアクセスするフロントエンドページを定義

ユーザ側に表示されるウェブページは，Microsoft .NET framework で提供されている System.Web.UI.Page クラスの派生クラスとして定義される．ウェブページのソースコードには，次のように記述した．

```
Public Class AtomWeb
    Inherits System.Web.UI.Page
 …（略）…
 Protected html As New Atom   ←　インスタンスの作成
 Private Sub Page_Load(…) Handles MyBase.Load
  html.Request = Me.Request   ←　プロパティにデータセット
  html.DataKeyValue= Me.Request.QueryString(“id”)
  html.ExecuteSelect()   ←　データベースへの閲覧メソッド
 …（略）…
 End Sub
End Class
```

このコードの動作を簡単に説明すると，Atom 型(元素のオブジェクト)の Protected 宣言オブジェクト変数として html という変数を定義し，インスタンスを初期化する．次に，定義した変数の Request プロパティに，Web サーバの環境変数や認証情報など格納されている Request オブジェクトのデータをセットする[9]．DataKeyValue プロパティには，オブジェクトの主キーを設定する．最後に，ExecuteSelect メッソドを実行することで，主キーの条件を満たす SELECT クエリーが自動生成され，データベースサーバから該当オブジェクトの情報を読み込みます．読み込まれ情報は，Hypertext クラスによって，html 言語として変換されウェブページとして表示されるようになっている．

公開，学認，開発用の目的の異なる 3 つの物理サーバは全て同一のコードで動作するようにした．クラスによる階層化によってソースコードの開発コストの軽減やメンテナンス性の向上を図った．アプリケーションによるセキュリティは，基底クラスに近い html_tool クラスに記述し，アプリケーション全体のセキュリティ機能の強化や新しい認証方式の導入を容易にできるようにした．

3.3 SharePoint サーバと研究型コンテンツサーバの連携

市販のグループウェアと独自開発をしたソフトウェアによって，利便性の高いサービスを展開することが期待される．本研究で使用した SharePoint サーバは，予定表，タスク管理，共有ドキュメント，アンケート，外部ページへのリンク機能などを持っており，グループ内の情報を事務的な情報を管理するためには，十分な機能を有している．また，研究型コンテンツサーバは，元素や化学種，研究ノートなどの様々な情報を取り扱うことができる．その 1 つの機能である研究ノートを例にとって，SharePoint サーバとの連携動作について説明する．図 4 に示す公開用サーバの画面には，2 つのリンクが設定されている．図 4-①に示す「学認共有 URL」は，学認ユーザによる共有サイトへの URL が記述できるようになっており，この公開サーバのコンテンツでは，SharePoint サーバのサイトがリンクされている．図 4-②には，「シボレスサイト」という表示で，リンクがされており，学認ログイン後，研究ノートの編集ページに遷移するようになっている．認証後の画面である図 4-③には，「編集メソッド」が追加表示され，編集画面に移動することができる．

学認用ウェブサーバと SharePoint サーバは，学認ログインによるシングルサインオンによって，一度の認証のみでそれぞれのサイトを利用することができる．市販のソフトウェアである SharePoint を利用することによって，定型化されたコンテンツは，使い勝手の良いユーザインターフェースで利用できるようにした. 研究型コンテンスサーバは，独自に開発によって，自由度の高い研究が取り扱う情報を容易に蓄積・発信できるようにした．これらの 2 つのサーバを相互にハイパーリンクし，かつ，学認ログインによるシングルサインオンによって，それぞれの持ち味を生かしたサービス展開を実現した．また，市販のグループウェアの機能を研究用コンテンツサーバ内に独自開発する場合，開発期間は 200 時間程度であると予想される．これら 2 つのサーバが連携することによって，低コストで利便性の高いサービスの提供が可能になる．

図 4　研究型コンテンツサーバと SharePoint サーバの連携

3.4 PKI 認証による電池状態の監視への試み

SAML ミドルウェアを使用した場合，ウェブサーバのシングルサインオンを導入することは可能である．一方，センサからの情報をサーバに送信し機械的に情報通信したい場合，SOAP や XML 通信の認証や暗号化に学認が利用できるようになれば，学術研究利用の幅が広がることが期待される．学認ログインとコンピュータ間で情報を共有できる XML 通信を利用した電池状態の監視システムへの試みについて紹介する．

電池寿命の予測には，電池の劣化状態を記録したデータベースより推測する方法が採用されているが，世界中の様々な電池の情報を収集・共有できるデータベースが存在しない．また，エネルギーと IT を融合した「スマートグリッド」は低炭素社会を実現するための取り組みとして，注目を受けている[10]．ビルなどで稼働している照明機器や空調機器のスマートグリッドのための共通通信プロトコル(CCP)の研究は行われているが，電池状態と監視するための CCP は検討されていない[11]．この試みでは，XML 言語によるスマートグリッドのために電池状態を監視する XML スキーマと学認ログインにある情報共有が可能性について検討した．

図 5 に学認によるスマートグリッドによる電池監視の概要を示す．主な課題は，「XML 通信のためのスキーマの設計」と「XML 通信時の認証」，「収集情報の共有方法」の 3 つである．

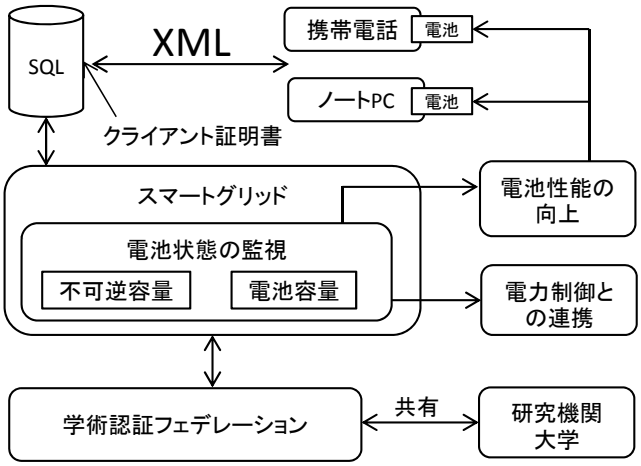

図 5　PKI 認証による電池状態の監視の概要

スキーマを設計するために，実際に携帯電話や懐中電灯などの負荷が有する充放電に関する情報の収集機能について調査した．その結果，放電容量や充電容量を計測する機能を有しているデバイスは少ないため，電池の充電を開始した日時を記録し，充電開始日時の間隔から電池の不可逆容量や電池容量を予測することが重要であると考えた．この仕様を満たすために必要な属性は，電池の ID，充電履歴の ID，充電開始日時であり，図 6 に示すような XML で記述することにした．

```
<?xml version="1.0" encoding="utf-16" standalone="yes"?>
<mydatabase>
<!--satart of document-->
  <Battery Object="urn:oid:1.3.6.1.4.1.22689.2.2.13">
    <id>12047</id> ←― 必須
    <caption>携帯電話の電池（テスト）</caption>
      <BatteryHistory Object="urn:oid:1.3.6.1.4.1.22689.2.2.62">
        <id>9218</id> ←― 必須
        <caption>ネット-[携帯電話の電池（テスト）]を使</caption>
        <StartDate Quantity="urn:oid:1.3.6.1.4.1.22689.2.1.8.551">2012-05-14T08:08:53.53Z</StartDate>
        <xQuantity szUnit="mol">0.07</xQuantity>
      </BatteryHistory>
      <BatteryHistory Object="urn:oid:1.3.6.1.4.1.22689.2.2.62">
        <id>9219</id>
    …
      </BatteryHistory>
  </Battery>
</mydatabase>
<!--end of document-->
```

必須

図 6　電池監視のための XML スキーマの例

XML 通信時の認証と暗号化については，クライアント証明書による PKI 方式を採用した．クライアント証明書は，本学の学術研究用の認証局および国立情報学研究所が運用している「eduroam 仮名アカウント発行システム」の認証局から発行されたものを使用できるようにした．PKI による認証と暗号化による携帯電話やパソコンの電池の充放電情報を安全に収集できるようになるであろう[12]．収集した情報の共有は，研究型コンテンツサーバの公開用ウェブサーバからの一部の情報を匿名ユーザに発信するようにした．また，匿名ユーザへの詳細情報の公開は非公開とし，学認ログインによる認証ユーザにのみ，詳細な情報を閲覧できるようにした．学認と PKI 認証による電池状態の監視により，電池をはじめとするエネルギーデバイスの開発と学問の発展寄与できることが期待される．

4. おわりに

市販のグループウェアである SharePoint サーバを ADFS サーバと連携することによって，学認に対応した．SharePoint サーバは，ドキュメントやスケジュール，タスクなどを共有する上では，便利なツールであった．しかし，数値や化学種，研究ノードなどを正規化して取り扱うためには，独自にデータベースとウェブサービスを開発する必要があり，研究型コンテンツサーバを開発した．研究型コンテンツサーバは，公開用と学認用の 2 つのウェブサーバを構築した．ウェブサーバのアプリケーションプログラムの開発を容易にするために，クラスによる階層化構造を導入した．階層化構造は，全体を同時に変更した場合，基底クラスに近いクラスを修正すること実現ができ，新しい認証方式への対応などが容易にできるようになるであろう．最後に，コンピュータ間における情報共有アプリケーションへの開発の 1 つとして，スマートグリッドのための電池状態の監視システムの構築を試みた．コンピュータ間の情報交換には XML 言語を採用し，クライアント証明書を使用した PKI 認証によって，携帯電話やパソコンなど電池の状態を安全に監視できるようになった．

本研究では，複数の SAML 対応ミドルウェアである ADFS と Shibboleth を使用して，市販のグループウェアと独自に開発したウェブサーバを組み合わせることにより，利便性の高い共有サービスを低コストで構築できた. また，XML 言語で記述したドキュメントオブジェクトをクライアント証明書によって認証・暗号化し，安全なコンピュータ間通信による情報収集を試みた.

今後，サービスプロバイダーを提供するときに，ADFS，Shibboleth，クライアント証明書を組み合わせることよって，開発期間を大幅に短縮して，利便性の高い学術コンテンツの共有サービスを提供できることが期待される. さらには，学術機関が運用する教育研究用データベースをお互いに活用することによって，学問の発展や真理の追究に貢献できることが期待される.

謝辞 Shibboleth および学認関連の質問にご回答いただきました国立情報学研究所および学認タスクフォースの皆様に深く感謝申し上げます．本学の認証情報の更新・管理にあたり，常に最新の情報に更新していただいた情報系センターのスタッフの皆様に深く感謝申し上げます．本サービスの一部の構築には，平成 22 年度国立大学法人設備整備費補助金事業の補助を受けて，実施した.

参考文献

1) UPKI イニシアティブ，https://upki-portal.nii.ac.jp/， (参照 2009-07-20).
2) 伊藤智博，吉田浩司，鈴木勝人，青木和恵：既存の複数認証基盤を統合した UPKI-SSO・eduroam 対応認証基盤の構築，平成 20 年シングルサインオン実証実験報告書 (2009).
3) 認証基盤も冗長構成化して可用性を向上，学認活用事例集，https://www.gakunin.jp/docs/fed/info， (参照 2012-02-09).
4) 学術認証フェデレーション，https://www.gakunin.jp/， (参照 2012-02-01).
5) 伊藤智博，高野勝美，田島靖久，吉田浩司：災害時に備えた分散キャンパスによる情報基盤の整備，学術情報処理研究誌，No. 15，pp. 5-11 (2011).
6) 伊藤智博：分散キャンパスを活用した複数 ISP 接続による eduroam アクセス回線の冗長化について，eduroam JP ケーススタディ，http://www.eduroam.jp/docs.html (参照 2011-06-10).
7) 伊藤智博，高野勝美，田島靖久，吉田浩司：複数 ISP と分散データベースによる高可用性認証連携サービスの構築，大学情報システム環境研究，Vol. 15，pp. 72-79 (2012).
8) 伊藤智博，立花和宏，奥山澄雄，高野勝美，田島靖久，吉田浩司：ADFS による学術認証フェデレーション対応 SharePoint サービスの構築，学術情報処理研究誌，No. 16，pp. 33-40 (2012).
9) HttpRequest クラス，http://msdn.microsoft.com/ja-jp/library/system.web.httprequest(v=VS.88).aspx, (参照 2012-09-18).
10) H. Tomihara, SURTECH Directory, p.29 (2009).
11) 東大のスマートグリッドを実現するグリーン東大の実証実験を聞く！， http://wbb.forum.impressrd.jp/feature/20100304/785， (参照 2012-07-02).
12) eduroam 仮名アカウント発行システム，https://eduroam-tmp.nii.ac.jp/，(参照 2012-09-05).